

SYSTEM AND METHOD FOR SELECTIVE COMMUNICATION SCANNING AT A FIREWALL AND A NETWORK NODE

5

ABSTRACT

A method and apparatus are provided for cooperatively and dynamically sharing a proxy's burden of scanning communications for target content. A network of computer nodes is connected to a firewall through which pass communications with entities external to the network. The firewall includes one or more proxies to facilitate network users' connections with the external entities. The firewall and one or more of the nodes include software modules for scanning one or more types (e.g., FTP, HTTP, SMTP) of communications for particular information or types of data (e.g., computer viruses, ActiveX components, pornography, text). A node having a software module for scanning a communication identifies its scanning capabilities to the firewall. The node may also suggest a class or set of communications that it may scan, which class or set may be defined by its operating parameters or attributes of communications received at the firewall for the node. The firewall negotiates with the node then specifies rules or criteria for determining which communications and under which circumstances the node may scan a communication instead of the firewall. When a communication is received at the firewall and is passed to the proxy, the proxy applies the specified rules to determine which of the proxy and the node should scan the communication. In this manner a substantial amount of communication scanning may be offloaded to individual computer nodes, thereby enhancing or avoiding degradation of the firewall's performance. The division of responsibility between the proxy and any node may be dynamically modified or re-negotiated at virtually any time according to any desired criteria or operating parameters.